Docket No. 1363-006 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
JOSEPH ANDREW MELLMER et al.	:	
Serial No.: 09/670,783	:	Group Art Unit: 2166
Filed: September 27, 2000	:	Examiner: Woo, Isaac M.

For: MANAGING DIGITAL IDENTITY INFORMATION

APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the Office Action of May 2, 2006, the Applicant hereby appeals the final rejection of claims 1, 3-58 and 90-101. Also, a Notice of Appeal accompanies this brief along with a fee transmittal indicating payment of the appropriate $500.00 Notice of Appeal fee and the $500.00 Appeal Brief fee set forth in 37 C.F.R. §§41.20(b)(1) and (b)(2), respectively.

I. Real Party in Interest

The real party in interest is Novell, Inc., a corporation of the State of Delaware, having a principal place of business at 1800 South Novell Place, Provo, Utah 84606.

II. Related Appeals and Interferences

The Appellant knows of no other prior or pending appeals, interferences, or judicial proceedings, which may be related to, directly affect, or be directly affected by, or have a bearing on, the Board's decision in this Appeal.

III. Status of Claims

All pending claims (1, 3-58 and 90-101) stand finally rejected under 35 U.S.C. §102(e) or §103(a). Namely, claims 90-101 stand rejected as anticipated in view of Dean et al. U.S. 6,023,762. Claims 1 and 3-58 stand rejected as obvious in view of Dean and French U.S. 5,794,228. Dean, however, is the primary patent upon which all rejections stand, with the exception that French is cited for the proposition of showing storage of multiple user objects for multiple users. Claims 2 and 59-89, on the other hand, have long ago been canceled. On appeal, the Appellant traverses the rejection of all pending claims. Claims 1, 90 and 98 are independent.

IV. Status of Amendments

No amendment has been filed subsequent to the Final Office Action dated May 2, 2006 and all previous amendments have been entered. The form of the claims for purposes

of appeal are those presented in the Amendment and Request for Continued Examination (RCE) filed by the Appellant on September 6, 2005 (received by the Patent Office on September 12, 2005) and re-presented for consideration in a Response filed by the Appellant on February 10, 2006 (received by the Patent Office on February 13, 2006). As required, a copy of the claims is included herewith in Appendix form with double-spacing format.

V. Summary of Claimed Subject Matter

Claims 1, 3-58 and 90-101 are pending. Claims 1, 90 and 98 are independent.

The present invention relates broadly to computers, especially server systems and storage media for managing and controlling personal, digital identity information of users. More particularly, the present invention contemplates a vault for storage of safes that, in turn, correspond with one or more user objects, each with one or more profiles. Access rights to these items, however, are apportioned to a system administrator to effectively manage the items (e.g., safes) in the vault while, at the same time, the profiles are accessed and administered exclusively by a user at the exclusion of the system administrator. In addition, the profiles are operable to be exchanged or shared with other users who, in turn, have their own profiles accessible and administered exclusively by themselves at the exclusion of the administrator. In this manner:

> tools and techniques [are provided] to manage digital (e.g., online or connectable) identity information to support policies and membership in communities. In various embodiments, it helps provide and maintain the integrity of relationships, and helps provide reliable information access, within a secured storage platform using an extensible schema. *Appellant's specification, p. 3, ll. 23-27.*

As identified in the background section of the specification, the foregoing is a needed solution to "reduce user tedium, to increase users' control over their private information, and to provide better ways to manage personal information according to the relationship of the parties involved." *Underlining added, Appellant's specification, p. 3, ll. 13-15.*

In general, computer system servers of the invention are found in operating environments 100, Figure 1, and includes or not individual computers, networks, servers, etc. 106, 108, 110, 112, 114. They are configured with appropriate hardware, software, combinations, etc. that are linked variously in infrastructure, such as via the Internet 104, for example, including or not various networked operating systems. *Appellant's specification, p. 9, l. 30 - p. 10, l. 27.*

The vaults 202 relate to that which stores one or more safes 200 of one or more users as representatively seen in Figure 2. Alternatively known as "vault objects" or "safe objects," as implemented in computer operating environments, for example, the "Safe objects and Vault objects are container objects" for containing other items. *Appellant's specification, p. 4, ll. 11-12.* That is, the vault "can hold Safe objects and other Vault objects." *Appellant's specification, p. 4, l. 18.* The Safe object, on the other hand, "belongs to and is managed by a particular . . . user." *Appellant's specification, p. 4, l. 12-13.* Among other things, it corresponds to user objects 308 representatively seen in Figure 3. In turn, the user objects 308 contain one or more profiles 300 particular to that user, e.g., "My hobby profile," "my biking profile," etc. A profile itself "can contain other profiles, e.g., Profiles 302, 304, 306" and, "for a given user[,] may contain distinct pieces of identity data, or they may share certain pieces of data, e.g., a user's work phone number." *Appellant's Specification, p. 13, ll. 15-19.* Ultimately, the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." *Appellant's specification, p. 13, ll. 23-25.* Figure

4 representatively shows John sharing a profile with Carol by way of representative access and contact lists 400, 402 for Carol and John, respectively.

In independent claim 1, and consistent with Figures 1-4, for example, the below-quoted limitations of the claim, in **bold**, are representatively found in the specification at the parenthetical cite as follows:

1. **A computer server system for managing digital identity information** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27*), **comprising at least one processor in operable connection with a memory configured by a database** ("*the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . .*" *Appellant's specification p. 10, l. 31 - p. 11, l. 3; and relative to Novell Directory Services (NDS) under the heading "NDS Software," for example, "[o]ne can create NDS objects for . . . databases . . ." Appellant's specification, p. 15, l. 17*), **the database including a vault for storage of multiple user objects for multiple users** *(vault 202 stores safes 200 and safes 200 correspond to user objects 308, for example, Figures 2 and 3, Appellant's specification p. 13, ll. 10-15*), **the vault having access rights granted to a system administrator for management of the multiple user objects** (*in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28*), **each of the user objects having a corresponding safe object** (*in one*

embodiment, "illustrated in Figure 8, a Vault account 800 includes the user object 308 and the Safe 200. Conceptually, the user object 308 belongs to and is managed by the Vault host 510. The host 510 can set the policy on the user object 308, e.g., by limiting the resources the user consumes. . . . The Safe 200 belongs to and is administered by the user, under the policy (such as space restriction) set by the host 510." Appellant's specification, p. 21, l. 23-28), **the safe object containing multiple different profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator** (*"The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17*), **each profile including digital identity information provided by the single one of the multiple users** ("*the summation of a person's personal data can be termed a 'digital identity.'" Appellant's specification p. 13, l. 1; "As there are many aspects of a person's real identity, there can also be many aspects of a . . . digital identity; these multiple aspects are called 'Profiles.'" Appellant's specification, p. 13., ll. 12-13*) **and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users** (*this architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." Appellant's specification, p. 13, ll. 23-25*), **the sharing occurring exclusively upon initiation by the single one of the multiple users** (*"In Figure 4, [for example] user Carol gives user John access by identifying John in an access list 400 and John includes Carol in his contact list 402. Carol defines the Profile . . . and grant[s] appropriate rights to the access structure 400." Appellant's specification, p. 13, ll. 25-28*).

In independent claim 90, the below-quoted limitations of the claim, in **bold**, are representatively found in the specification at the parenthetical cite as follows:

90. **A computer server system for managing digital identity information** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27*), **comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities** ("*the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . .*" *Appellant's specification p. 10, l. 31 - p. 11, l. 3*), **the vault including an access protocol layer, an identity server layer and an identity manager layer** (*"The identity Vault 202 provides storage of, and controlled access to, the identity data. In one embodiment, the identity Vault 200 is defined in three layers as illustrated in Figure 7, namely, an access protocol layer 700, an identity server layer 702, and an identity manager layer 704." Appellant's specification, p. 19, l. 30 - p. 20, l. 2*) **and having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users** (*in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28*), **the one or more safes of digital identities having multiple profiles each with access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of**

the one or more system administrators (*The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17*), **the multiple profiles being shared amongst the end users at the exclusion of the one or more system administrators** (*the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." Appellant's specification, p. 13, ll. 23-25. Figure 4 representatively shows John sharing a profile with Carol by way of representative access and contact lists 400, 402 for Carol and John, respectively.*).

In independent claim 98, the below-quoted limitations of the claim, in **bold,** are representatively found in the specification at the parenthetical cite as follows:

98. **A configured computer-readable storage medium that manages digital identities** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27; and the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . ." Appellant's specification p. 10, l. 31 - p. 11, l. 3*), **comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer** (*"The identity Vault 202 provides storage of, and controlled access to, the identity data. In one embodiment, the identity Vault 200 is defined in three layers as illustrated in Figure 7, namely, an access protocol layer 700, an identity server layer 702, and an identity manager layer 704." Appellant's specification, p. 19, l. 30 - p. 20, l. 2*) **and having access rights granted to a system administrator for management of the safes of digital identity**

profiles (*in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28*), **the one or more safes of digital identity profiles having access rights granted exclusively to one or more end users at locations remote from the vault** (*The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17; end users are remote from the vault in any of a variety of instances in Figure 1, for instance*), **the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator** (*the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." A profile itself "can contain other profiles, e.g., Profiles 302, 304, 306" and, "for a given user[,] may contain distinct pieces of identity data, or they may share certain pieces of data, e.g., a user's work phone number." Appellant's Specification, p. 13, ll. 15-19. Appellant's specification, p. 13, ll. 23-25. Figure 4 representatively shows John sharing a profile with Carol by way of representative contact lists 400, 402 for Carol and John, respectively.*).

VI. Grounds of Rejection to be Reviewed on Appeal

A. The Board must determine whether claims 90-101 are rendered anticipated under 35 U.S.C. §102(e) in view of Dean and whether claims 1 and 3-58 are further obvious (35 U.S.C. §103(a)) over Dean in view of French. **Dean, however, is the primary patent upon which all rejections stand, with the exception that French is cited for the proposition of showing storage of multiple user objects for multiple users**. Thus, the overarching question is whether Dean shows the aspects the Examiner contends it does.

In this regard, the Board must essentially determine: A) whether Dean teaches identity profiles in a safe, in turn, in a vault, with access to manage the vault extending to a system administrator while access and administration rights of the profiles extend to users ***at the exclusion of the system administrator***; B) whether Dean has abstraction layers, such as an identity server layer, an access protocol layer and an identity manager layer thereby defining a vault, especially a vault for storing safes, in turn, storing profiles with access to manage the vault extending to a system administrator while access and administration rights of the profiles extend to users at the exclusion of the system administrator; C) whether Dean and French are properly combined; and D) whether the Examiner has met his *prima facie* burden.

To the extent the Board's determination finds any of the above in favor of the Appellant, the entirety of the claims should be adjudicated patentable in view of the pending rejections.

B. While not a ground of rejection, the Appellant also requests the Board to review the administrative handling of this file by the Examiner. This matter had its original claims rejected as obvious over Chang 6,157,953 in view of Van Dyke 6,412,070. According to the Examiner, Chang included all the elements of the independent claims with the exception that Van Dyke (relative to claims 1-58) incorporated "having access rights granted to a system administrator, operable to be shared with other users having' [sic] other profiles

accessible and administered exclusively by the other users, the string occurring exclusively upon initiation by the user." *Underlining added, Page 4, 1st ¶, 4-19-05 Final Rejection.* As is clear, the Examiner issued a Final Rejection on an erroneous record built on non-existent claim limitations about "the string" of something. Although the Applicant sought clarity, an Advisory Action issued and reiterated the notion of "the string."

After filing an RCE, to meet various timing obligations and including further clarification regarding "the string," the Examiner completely abandoned the Chang and Van Dyke references in lieu of the now-cited Dean and French references. As it relates to the claims, they have never been amended other than to reflect the nature of interaction of multiple users with multiple profiles, etc. Since adding aspects of multiplicity to the claims, it seems the Examiner's prior searching should have remained relevant and the Dean and French references certainly should have already been of record from prior searches and/or applied. The Chang and Van Dyke references should have also certainly been applicable to the Examiner's prior line of reasoning. However, no explanation has ever been given regarding the abandonment of Chang and Van Dyke in favor of Dean and French. Despite repeated attempts to build an appropriate record regarding "the sharing" of profiles, and not "the string," nothing has ever been advanced by the Examiner. The Appellant does not mind a thorough prosecution by the Examiner, however, prosecution has progressed confusingly for reasons unbeknownst to the Appellant. Also, while the cost of prosecution is fairly expensive in modern times, the cost in this matter has progressed seemingly unfairly relative to a confusing record. As can be appreciated, the burden to continually fend off imprecise reasoning is overly costly in time, effort and money to both the Appellant and the Patent Office.

VII. Argument

A. The Appellant offers the following preliminary remarks in consideration of its arguments.

1. Brief Background of Dean U.S. Patent No. 6,023,762

Dean teaches callers (e.g., boss, colleague, wife, self, etc.) able to access remote data of users (e.g., employee info 200, project info 201, private info 202, etc.) apportioned amongst various "data views." Via the functionality of a gatekeeper, described as an Agent, e.g., 107, callers make requests for the data and, if authenticated, the agent returns the requested data. In this regard, the agent 107 "allows or denies access to portions of data stored in the user data sources depending upon who is requesting the information and the type of data requested to be accessed." *Col. 4, ll. 39-42.* In various embodiments, the components enabling this functionality generally include an authorization decoder 400, a look up table 401, and a data access/retrieval signal generator 402. In turn, the look up table 401 is a "data structure" comprising:

> types of callers who may request information from the user database, and for each caller type, sets of data files or types of data files in the user data sources which can be accessed by that category of caller, together with a corresponding authentication method, corresponding to a respective level of authentication. *Col. 5, ll. 41-47.*

Naturally, portions or entireties of the underlying "information from the user database," such as "personal medical information and personal financial results" (*col. 5, l. 67 - col. 6, l. 1*), is populated by the user himself or herself.

2. Brief Background of French U.S. Patent No. 5,794,228

French teaches a "Client/Server Database System with improved methods for performing database queries, particularly DSS [Decision Support Systems 240]-type queries." *Col. 3, ll. 10-12.* In various embodiments, concatenated data pages 310, 320, 330 of cells of columns in a table 300 are "optimized for compression" via storage of various status flags that indicate "whether the data page is a candidate for compression and (optionally) what type of compression is best suited for the data on that page." *Col. 4, ll. 18-22.* User information, such as name, street, city, etc., is a representative form of the data in the column and rows of the table, e.g., Figure 3A.

B. Unlike the present invention, Dean never identifies profiles in a safe, in turn, in a vault, with access to manage the vault extending to a system administrator while access and administration rights of the profiles are extended to users at the exclusion of the system administrator.

Although variously worded, the instant invention requires profiles in safes in vaults, with access rights of the vaults extending to the system administrator. At the same time, access rights of the profiles extend to the users, at the exclusion of the administrator. Ultimately, the profiles are for sharing with other users (who also have profiles administered by themselves at the exclusion of the administrator).

In the rejections, the Examiner cites the Dean reference for the proposition of the foregoing features of the invention. Among other things, it is contended that "having access right [sic] granted to one or more system administrators" occurs in Dean according to "(security level, col. 4, lines 33-40, authentication level, fig. 3)." *5-2-06 Final Office Action, p. 4, final paragraph (in rejecting claims 90-101).*

In its entirety, Dean states at this cite:

> Such user information may have various levels of security, and a user may wish to restrict access to such information depending upon who is requesting that information. A plurality of callers operating key devices access the user data sources by addressing the agent 107. Access to user data describing the user information is controlled by the electronic agent device 107 which allows or denies access to portions of data stored in the user data sources depending upon who is requesting the information and the type of data requested to be accessed. *Dean, col. 4, ll. 33-42.*

To the extent the Examiner likens Dean's agent 107 to the claimed system administrator, the Dean agent 107, in contrast to the invention, **has access** to the underlying data of users being requested by callers. At Dean's step 606, Figure 6, for example, and via the functionality of the Data Access/Retrieval Signal Generator 402, the agent 107 actually does the sending of the "requested info over WAN." As more precisely stated at *col. 7, ll. 54-57*, if the agent authorizes the caller, "in step 606, the authentication decoder authorizes the data retrieval signal generator ***to access the information from the user data sources*** to be sent to the service terminal [of the caller making the request]." In other words, Dean's agent simply keeps a protective gate in front of the underlying data to prevent unauthorized callers from having access to it. But, to the extent the callers have an appropriate level of access, and it can be authenticated, the agent indeed fetches the underlying data and gives it to the callers. This is hardly, then, the "exclusion" of a system administrator from underlying data in profiles, in safes, in vaults as the claims of the invention require.

Similarly, the "exclusive" administration by users in claims 1 and 3-58 is purportedly found in Dean by the following: "(each user, without the system administrator, configures look-up table [sic] (for safe object access))." *5-2-06 Office Action, p. 9, ll. 16-17.* The Applicant, however, does not dispute Dean teaches users configuring underlying information

in a look up table. But, to suggest that Dean's system administrator, to the extent an agent 107 is arguably a system administrator, anticipates or in combination with French renders the claims of the invention obvious, is failure as a matter of law.

In additional embodiments of Dean, Figures 7 and 10 teach other agents as elements 702 and 1000. These too, however, teach access to underlying information contrary to the claimed limitations of a system administrator not having access to underlying data of profiles. That is, Agent 702 interfaces with user databases 704, 705 and sends "information/service data" directly to the service terminal 701. As described in the specification:

> [w]here authorization is successful, the agent allows access to user data sources containing data as described in the look-up table 401. For example, a caller who has been successfully identified as a co-worker may have access to diary information or project information. . . .***User data sources respond by transmitting the requested user data to the agent. The agent relays the communications signals comprising user data or service data*** on to the service terminal, and it is received by the service terminal in step 808. *Emphasis added, Dean's specification, col. 8, ll.48-52 and ll. 57-61.*

Relative to Figure 10, the firewall device 1001 "retrieves the user data from the protected user sources, and ***relays the user data to the agent device [1000].***" *Emphasis added, Dean's specification, col. 9, ll. 26-28.* In other words, the agents of Dean, especially agent 107, agent 702 or agent 1000, always have access to the user data of the users.

At a minimum, the Examiner's position is either 1) plausible only upon a further, forthcoming explanation, e.g., such as by an explanation how the explicit statements that an agent has access to user data is somehow not access to the user data, or 2) is a disingenuous attempt to equate a reference to the claims where no equation exists. As before, nowhere does Dean suggest that its agent is excluded from information of the look up table. In fact, the exact converse is true. Also, the Examiner has never clarified the record as to why an

agent of Dean should even be equated to a system administrator of the claims. For at least these reasons, the claims define over the art of record.

C. Dean has no abstraction layers defining a vault, such as an identity server layer, an access protocol layer and an identity manager layer, much less a vault defined by these layers for storing safes, in turn, for storing profiles with access to manage the vault extending to a system administrator while access and administration rights of the profiles are extended to users at the exclusion of the system administrator.

In independent claims 90 and 98, a vault includes "an access protocol layer, an identity server and an identity manager layer." The Examiner rejects the claims, however, by making associations to Dean that, quite frankly, do not exist anywhere in the teachings. For example, the Examiner rejects claims 90-101 by associating the "identity server layer" of the claims with Dean's element 803, Figure 8. *See, 5-2-06 Final Office Action, page 4, final paragraph.* However, element 803 of Figure 8 recites a step of a service terminal as "Send terminal ID signal to key device." Without a doubt, this does not equate to a precisely claimed software abstraction "identity server layer," especially one in a "vault" further including "an access protocol layer . . . and an identity manager layer."

Even assuming the Examiner's cite to Dean's sending a terminal ID signal to a key device, element 803, corresponds to an abstracted identity server layer of the claims (and the Appellant does not admit this), the Dean element does not define a vault, much less one further including an access protocol and an identity manager layer. For example, Dean's element 803 unequivocally relates to the Service Terminal 701 and its relationship with the Key Device 703, e.g., Figure 7. However, the data of Dean, e.g., employee info 200, project info 201, private info 202, etc., which is configured by users and stored in databases, such

as databases 704, 705, is found behind the functionality of the Agent 702, not in the Keying Device 703. In other words, if the Examiner's position that the login/ID relationship between the Service Terminal 701 and the Keying Device 703 defines an abstract layer as part of a vault storing data, the Service Terminal 701 and the Keying Device 703 must then together be the vault in which the user data is stored. Yet, it is not. As is clear, the user data is stored in databases 704, 705 that is gateway-accessed through an agent 702 from callers with a keying device 703. Nowhere is user data ever stored in apportioned functionality between the Keying Device and the Service Terminal.

Similarly, the Examiner cites the claimed "access protocol layer" of the vault as "fig. 1, TCP/IP, col. 3, lines 27-65." *5-2-06 Final Office Action, p. 4, final paragraph.* However, if the TCP/IP element 104 of Figure 1 is a layer of a vault, then it too must be part of an element that stores the underlying data of the users. However, Dean's TCP/IP element 104 nowhere stores data of the users. Rather, it is the database 105 protected by the Agent 107 of the Corporate WAN that stores the data in Figure 1.

Relatedly, the Examiner cites the claimed "identity manager layer" of the vault as Dean's elements "805, 806, authorization service, fig. 8, col. 8, lines 1-39." *5-2-06 Final Office Action, p. 4, final paragraph.* However, Dean's elements 805 and 806 relate to the interchange/interface between the Service Terminal 701 and the Agent 702 and such does not ultimately store the underlying data of users. Instead, the user data is stored in databases 704, 705 on a side of the Agent 702 opposite the side of the Agent interfacing with the Service Terminal 701. For at least these reasons, the claims are patentable over Dean and/or its combination with French.

What appears to be happening is an Examiner oversimplifying the claim limitations. That is, the Examiner seems to hodgepodge together any element that teaches a protocol, any element that teaches identification, any element that teaches storage, and any element that

teaches user data and then concludes anticipation or obviousness in view thereof. However, the instant invention is a precise arrangement of elements that is not found in the Examiner's mishmash of elements. Namely, claims 90 and 98 require an interaction that the three layers together, e.g., the access protocol, the identity server and the identity manager, define the vault that store the profiles of users, wherein the vault has access rights granted to a system administrator while the profiles have rights that exclude the system administrator. For at least these additional reasons, the claims are patentable over Dean and/or its combination with French.

D. Even if Dean and French are properly combined, and the Appellant contends they are not, the two references do not result in the instant invention.

From above, Dean teaches callers (e.g., boss, colleague, wife, self, etc.) able to access remote data of users (e.g., employee info 200, project info 201, private info 202, etc.) apportioned amongst various "data views." Via the functionality of a gatekeeper, described as an Agent, callers make requests for the data and, if authenticated, the agent returns the requested data.

French, on the other hand, teaches a "Client/Server Database System with improved methods for performing database queries, particularly DSS [Decision Support Systems 240]-type queries." *Col. 3, ll. 10-12.* In various embodiments, concatenated data pages 310, 320, 330 of cells of columns in a table 300 are "optimized for compression" via storage of various status flags that indicate "whether the data page is a candidate for compression and (optionally) what type of compression is best suited for the data on that page." *Col. 4, ll. 18-22.*

To the extent Dean and French are combined, the result is compression/de-compression of the data of users that is gateway-accessed by the interaction of Dean's Agent. In other words, the combination yields the agent-as-gateway feature of Dean with the data compression/de-compression features of French. Nowhere does this relate to the functionality of the instant invention whereby vaults store profiles of users with rights of the vault extending to system administrators while rights of the profiles exclude the system administrator. It certainly does not result in vault layers, the sharing of profiles or other features of the various claims.

As the law has long held, the proper test of obviousness is whether the differences between the invention and the prior art are such that "the subject matter as a whole would have been obvious at the time the invention was made" to a person skilled in the art. *Stratoflex Inc. V. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983)(Underlining added). Bear in mind, the Applicant originally filed this application for patent protection on September 27, 2000. It is now over five full years since filing. The Applicant also reminds of the caution expressed by the Court of Appeals for the Federal Circuit that "[d]etermination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the [] invention." *ATD Corp. v. Lydall, Inc.*, 159 F.3d 534, 536 (Fed. Cir. 1998).

However, it appears the Examiner position of obviousness is nothing more than the cautioned-against selective culling from the references in an attempt to fit the limitations of the claims. Not that the Examiner has fit the limitations, but rejections of this sort are clearly discouraged under the law.[1]

---

[1]As is well established, "virtually all [inventions] are combinations of old elements." *Ruiz v. A.B. Chance Co.*, 69 USPQ2d 1686, 1690 (Fed. Cir. 2004). Also, an obvious determination under 35 U.S.C. 103(a) requires an "as a whole" analysis of the prior art to otherwise prevent an

E. The Examiner Fails to Meet his Burden of Establishing Obviousness

As longstanding precedent, the initial burden of establishing a prima facie basis to deny patentability to a claimed invention on any ground is always on the examiner. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). However, it appears the Examiner's legal position in the instant matter relates exclusively to Dean teaching/disclosing the entirety of all the pending claim elements with the exception that French provides the teaching "data storage . . . for multiple users." *5-2-2006 Final Office Action, p. 9, final three lines.* For several reasons, this rationale is flawed and insufficient.

First, the Examiner asserts the motivation or suggestion to combine Dean and French relates to the nature of the problem to be solved. Namely, the motivation to combine relates to "provid[ing] Dean's system the capability of storing multiple user objects to effectively share and manage user's information with other users in multi-user sharing network environment." *5-2-2006 Final Office Action, p. 10, ll. 5-7.*

Dean, however, already accounts for scenarios of multi-user environments and need not look to French, for any reason.

Second, the Appellant agrees the law allows for examining the nature of the problem to be solved when determining motivation.[2] However, the instant invention does not simply

---

impermissible "evaluation of the invention part by part." *Id.* For otherwise, "an obviousness assessment might break an invention into its component parts (A+B+C), then find a prior art reference containing A, another containing B, and another containing C, and on that basis alone declare the invention obvious." *Id.* In turn, "this form of hindsight reasoning, using the invention as a roadmap to find its prior components, would discount the value of combining various existing features or principles in a new way to achieve a new result - often the very definition of invention." *Id.*

[2] "A suggestion or motivation to modify prior art teachings may appear in the context of the public prior art, in the nature of the problem addressed by the invention, or even in the knowledge of one of ordinary skill in the art."

address solving a problem in a multi-user environment. Rather, the instant invention broadly relates to "better ways to manage personal information on the Internet," for example, to overcome the problems identified in the prior art. *Appellant's specification, p. 3, l. 12.* More narrowly, the instant invention relates to managing this information "according to the relationship of the parties involved," (*Appellant's specification, p. 3, l. 15*), especially via the "access rights given to a system administrator [of a vault and] . . . profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator."[3] Ultimately, it is overstated to simply characterize the nature of the problem to be solved as relating to "multiple user environments" because the claims are themselves much more narrow in focus and relate precisely to the relationships of the parties involved in the multi-user environment.

Third, the Court of Appeals for the Federal Circuit has warned that, "***simply identifying all of the elements in a claim in the prior art does not render a claim obvious.***" *Ruiz*, 357 F.3d at 1275. Some quantum of proof is certainly required. *Id.* To the extent the Examiner has identified all the elements of any one claim, although the Appellant strongly asserts this has not occurred, the Examiner has so far only offered proof of motivation to combine Dean and French by contending (without substantiation) that "it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Dean by incorporating storage of multiple user objects for multiple users with system of French . . . [for] provid[ing] Dean's system the capability of storing multiple user objects to effectively share and manage user's information with other users in multi-user sharing

---

Underlining added, Princeton Biochemicals, Inc. Beckman coulter, Inc., 04-1493, 6/9/2005, 411 F.3d 1332 (Fed. Cir. 1995).

[3] The selected language here comes from claim 1. Of course, the other claims have similar, but varied limitations and the variations of any given claim control its scope.

network environment." *5-2-2006 Final Office Action, p. 10, ll. 1-7.* However, this assertion is rawly given and merely represents what the Examiner thinks a skilled artisan would have thought about the instant invention nearly six years ago, to the extent French, for example, is even at all relevant to the instant invention. It is also a scant assertion with little, if any, underlying support.

F. Conclusion

The Appellant submits that (1) all claims are in a condition for allowance; (2) that Dean does not anticipate; and (3) that the combination of Dean and French does not render obvious. Accordingly, it is respectfully requested that the rejections of the pending claims be reversed and the application be remanded to the Examiner for allowance.

To the extent any fees are due beyond those authorized in the originally filed fee transmittal for filing a Notice of Appeal and brief in support thereof under 37 C.F.R. §§41.20(b)(1) and (b)(2), the undersigned authorizes their deduction from Deposit Account No. 11-0978.

Respectfully submitted,

KING & SCHICKLI, PLLC

Michael T. Sanderson
Reg. No. 43,082

247 North Broadway
Lexington, KY 40507
(859) 252-0889

Certificate of Mailing

I hereby certify that this correspondence having 39 total pages is being deposited with the United States Postal Service as first class postage pre-paid mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 29, 2006

Date 6/29/06 by

VIII. CLAIMS APPENDIX

The claims on Appeal include 1, 3-58 and 90-101. Of those, claims 1, 20, 25, 49, 50, 58, 90, 98 and 101 appear as previously presented while all others remain as originally presented. Claims 2 and 59-89 remain canceled.

The Listing of Claims:

1. (Previously Presented) A computer server system for managing digital identity information, comprising at least one processor in operable connection with a memory configured by a database, the database including a vault for storage of multiple user objects for multiple users, the vault having access rights granted to a system administrator for management of the multiple user objects, each of the user objects having a corresponding safe object, the safe object containing multiple different profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users, the sharing occurring exclusively upon initiation by the single one of the multiple users.

2. (Canceled)

3. (Original) The system of claim 1, wherein the safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles.

4. (Original) The system of claim 1, wherein the safe object also contains at least one drop box object.

5. (Original) The system of claim 1, wherein the safe object also contains at least one application object with settings for an application.

6. (Original) The system of claim 1, wherein the safe object also contains at least one view object.

7. (Original) The system of claim 1, wherein the safe object also contains at least one access object.

8. (Original) The system of claim 1, wherein the system comprises a web server and an identity server.

9. (Original) The system of claim 8, wherein the web server and the identity server communicate using encrypted usernames.

10. (Original) The system of claim 8, wherein the web server and the identity server are secured by a firewall.

11. (Original) The system of claim 1, wherein the system comprises an identity server appliance.

12. (Original) The system of claim 1, further comprising a zero-byte client.

13. (Original) The system of claim 1, further comprising an installed client.

14. (Original) The system of claim 1, wherein the system comprises a provider model for access to the database, and the provider model abstracts the details of a particular directory and storage protocol.

15. (Original) The system of claim 1, wherein the system comprises an abstract model for access to the database, and the abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data.

16. (Original) The system of claim 1, wherein the system comprises a programmatic interface to identity items and operations that correspond generally to directory service objects.

17. (Original) The system of claim 1, wherein the database includes multiple safe objects contained in a vault object.

18. (Original) The system of claim 17, wherein the system includes at least two vault objects hosted on different servers, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers.

19. (Original) The system of claim 18, wherein the objects are federated using a Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object.

20. (Previously Presented) The system of claim 1, further comprising a digital business card application object having a corresponding profile object which includes digital identity information provided by the single one of the multiple users.

21. (Original) The system of claim 1, wherein the system comprises a means for one user to receive updated profile information of another user using a link to the database.

22. (Original) The system of claim 1, wherein the database is a partitioned directory services database.

23. (Original) The system of claim 1, wherein the system is further characterized in that it provides an account creation service which creates a new account for a user based on a template.

24. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe management service which provides an administrative tool to manage and maintain safe objects.

25. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it provides a schema management service which permits the system

25. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it provides a schema management service which permits the system administrator to at least view a directory service schema.

26. (Original) The system of claim 1, wherein the system is further characterized in that it provides a batch account creation service which creates several accounts at one time.

27. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which permits one to install and configure an identity server.

28. (Original) The system of claim 1, wherein the system is further characterized in that it provides a backup and restore service which allows one to backup and restore at least one safe object.

29. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe advisor service which allows one to verify the integrity of a safe object.

30. (Original) The system of claim 1, wherein the system is further characterized in that it provides a legal recovery tool which recovers digital identity information for forensic use.

31. (Original) The system of claim 1, wherein the system is further characterized in that it provides a data denormalization service which facilitates data transformation on database fields.

32. (Original) The system of claim 1, wherein the system is further characterized in that it provides a rules service.

33. (Original) The system of claim 1, wherein the system is further characterized in that it provides an event service which allows an identity server to register interest in and be notified of changes in the database.

34. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity verification service which allows one to verify the identity of a user based on registration information.

35. (Original) The system of claim 1, wherein the system is further characterized in that it provides an authorization service which allows a process to verify information gathered from a user registration form.

36. (Original) The system of claim 1, wherein the system is further characterized in that it provides a profile discovery and publishing service which allows users to publish at least a portion of their profile information.

37. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form fill-in service which allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects.

38. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form conversion service which assists a webmaster in converting existing forms to standardized field names.

39. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which installs servlets on a web server.

40. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity exchange service for portions of a privacy protection protocol.

41. (Original) The system of claim 1, wherein the system is further characterized in that it provides a chat service which sets up chat rooms so users can communicate with each other in real time.

42. (Original) The system of claim 1, wherein the system is further characterized in that it provides a presence service which lets users specify where they are and allows them to discover another user's presence information.

43. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous remailer service which allows users to choose different email addresses for different profiles.

44. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information.

45. (Original) The system of claim 1, wherein the system is further characterized in that it provides an infomediary service which facilitates creating an infomediary.

46. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and software for tracking IP addresses in order to selectively publish the last known IP address of a user.

47. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and at least one of an underlying directory service and an underlying file system in order to enforce access controls on web pages published by users.

48. (Original) The system of claim 1, wherein the system is further characterized in that it provides email services.

49. (Previously Presented) The system of claim 48, wherein the single one of the multiple users has an email address, and the system encodes contact relationship information in the email address.

50. (Previously Presented) The system of claim 48, wherein the system uses profiles to filter email sent to the single one of the multiple users.

51. (Original) The system of claim 1, further comprising a means for determining whether a user logging in at a third party web site is registered as a user of the system.

52. (Original) The system of claim 51, further comprising a means for logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered.

53. (Original) The system of claim 52, wherein the means for registering the user and logging the user in comprises a means for capturing user login information for the third party web site.

54. (Original) The system of claim 1, wherein the system is further characterized in that user digital identity information is only made available to a partner site if the user has flagged the information as public.

55. (Original) The system of claim 1, wherein the system is further characterized in

that it uses an embossed icon which provides a transaction history.

56. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a user authentication mechanism.

57. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a launch point for launching application programs.

58. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it uses a non-repudiation feature whereby the system administrator cannot change a user password and then log on as the user.

Claims 59-89 (Canceled)

90. (Previously Presented) A computer server system for managing digital identity information, comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities, the vault including an access protocol layer, an identity server layer and an identity manager layer and

having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users, the one or more safes of digital identities having multiple profiles each with access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators, the multiple profiles being shared amongst the end users at the exclusion of the one or more system administrators.

91. (Original) The system of claim 90, wherein the access protocol layer includes one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP.

92. (Original) The system of claim 90, wherein the identity server layer serves as an NDS access point.

93. (Original) The system of claim 90, wherein the identity server layer maintains access rights to the digital identities.

94. (Original) The system of claim 90, wherein the identity manager layer includes NDS authentication and authorization that controls access to the digital identities.

95. (Original) The system of claim 90, wherein the identity manager layer has a secret store.

96. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are located on an identity server.

97. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are functionally apportioned between a client, a web server and an identity server, including servlets and applets.

98. (Previously Presented) A configured computer-readable storage medium that manages digital identities, comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to a system administrator for management of the safes of digital identity profiles, the one or more safes of digital identity profiles having access rights granted exclusively to one or more end users at locations remote from the vault, the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator.

99. (Original) The configured storage medium of claim 98, further including a zero-byte client interface.

100. (Original) The configured storage medium of claim 98, further including a client application interface.

101. (Previously Presented) The configured storage medium of claim 98, further including a database including a user object and a corresponding safe object, the safe object containing at least one profile of the digital identity profiles.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None